Title (en)

MEMORY-EFFICIENT HARDWARE CRYPTOGRAPHIC ENGINE

Title (de)

SPEICHEREFFIZIENTE HARDWARE-KRYPTOGRAPHIEMASCHINE

Title (fr)

MOTEUR CRYPTOGRAPHIQUE MATÉRIEL À MÉMOIRE EFFICACE

Publication

EP 3803672 B1 20240207 (EN)

Application

EP 19727684 A 20190529

Priority

- GB 201808834 A 20180530
- EP 2019064108 W 20190529

Abstract (en)

[origin: WO2019229192A1] A hardware cryptographic engine (8) comprises a direct-memory-access (DMA) input module (13) for receiving input data over a memory bus, and a cryptographic module (15). The cryptographic module (15) comprises an input register (20) having an input-register length, and circuitry (22) configured to perform a cryptographic operation on data in the input register (20). The hardware cryptographic engine (8) further comprises an input-alignment buffer (16) having a length that is less than twice said input-register length, and alignment circuitry (23) for performing an alignment operation on input data in the input-alignment buffer(16). The hardware cryptographic engine (8) is configured to pass input data, received by the DMA input module (13), from the memory bus (10) to the input register (20) of the cryptographic module (15) after buffering an amount of input data no greater than the length of the input-alignment buffer (16).

IPC 8 full level

G06F 21/72 (2013.01); **G06F 21/74** (2013.01)

CPC (source: EP US)

G06F 13/28 (2013.01 - US); **G06F 21/72** (2013.01 - EP US); **G06F 21/74** (2013.01 - EP); **H04L 9/06** (2013.01 - US); H04L 2209/12 (2013.01 - US)

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

WO 2019229192 A1 20191205; CN 112513856 A 20210316; EP 3803672 A1 20210414; EP 3803672 B1 20240207; GB 201808834 D0 20180711; US 12010209 B2 20240611; US 2021216665 A1 20210715

DOCDB simple family (application)

EP 2019064108 W 20190529; CN 201980049863 A 20190529; EP 19727684 A 20190529; GB 201808834 A 20180530; US 201917059393 A 20190529